

# UNITED STATES DISTRICT COURT

for the  
District of South Carolina

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Residence located at 104 Crest Street, Simpsonville,  
South Carolina,

Case No. 6:19CR385

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the \_\_\_\_\_ District of \_\_\_\_\_ South Carolina \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

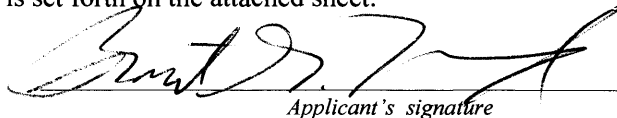
Code Section  
18 U.S.C. § 2252A

Offense Description  
Possession of Child Pornography

The application is based on these facts:

See attached affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

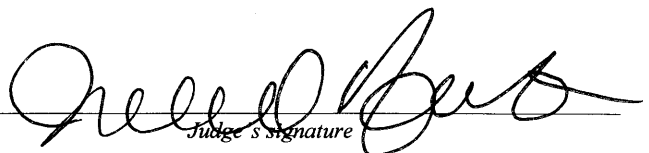
Robert G. Hamod Special Agent FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 04/05/2019

City and state: Greenville, SC



Judge's signature

JACQUELYN D. AUSTIN, U.S. Magistrate

Printed name and title

**A F F I D A V I T**

I, ROBERT G. HAMOD, being duly sworn hereby depose and state:

I am a duly appointed Special Agent of the FBI currently assigned to the Greenville, South Carolina, Resident Agency and have been so employed for the past twenty-seven years. Upon accepting a position with the FBI, your affiant underwent an extensive sixteen week training course involving investigations of federal crimes, to include Interstate Transportation of Child Pornography. Your affiant has personally been involved with the investigation of Steven Melton, in the [REDACTED], South Carolina area involving the transportation and possession of child pornography. The statements contained in this affidavit are based in part on information provided by a Confidential Human Source (CHS) of the Columbia Division of the FBI and on my experience and background as a Special Agent of the FBI. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Section 2252A are located [REDACTED] [REDACTED], South Carolina.

## STATUTORY AUTHORITY

This investigation concerns alleged violations of Title 18, United States Code, Sections 2252A(a)(1) and 2252A(a)(5)(B), concerning the transportation and possession of material constituting or containing child pornography and 2251(a), concerning enticing a minor to engage in sexually explicit conduct (as defined in 18 U.S.C § 2256(2)) for the purpose of producing a visual depiction of such conduct, knowing such conduct would be transported in interstate commerce.

## COMPUTERS AND CHILD PORNOGRAPHY

Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which persons whom have a sexual interest in children interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public.

The distribution of these wares was accomplished through a combination of personal contact, mailings and telephone calls. Any reimbursement would follow these same paths.

The development of computers has changed all of this. Computers serve four functions in connection with child pornography. These are: production, communication, distribution, and storage.

Pornographers can now produce both still and moving images directly from a common digital camera or web camera. The camera is attached, using a cable, directly to the computer. This turns the video output into a form that is usable by computer programs. The output of the camera can be stored, manipulated, transferred or printed out directly from the computer. The captured image can be edited in very similar ways to a photograph. The image can be lightened, darkened, cropped, and manipulated in a wide variety of ways. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. There is the added benefit to the pornographer that this method of production does not leave as large a trail for

law enforcement to follow as have methods that have been used in the past.

Previously, child pornographers had to rely on personal contact, U.S. Mail, and telephonic communications in order to sell, trade, or market pornography. The development of the computer has also changed that. A device known as a modem allows any computer to connect to another computer through the use of cables, fiber optic lines or telephone lines. By connection to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a dedicated network and serves many users. These host computers are sometimes commercial concerns, such as Charter Communications or AT&T Internet Services which allow subscribers to use either cable or telephone lines to connect to a network which is in turn connected to their host systems. These service providers allow electronic mail service between subscribers and sometimes between their own subscribers and those of other networks. Some of these systems offer their subscribers the ability to communicate publicly or privately with each other in real time in the form of "chat rooms." Contact with others in this online format can be either very open and anonymous, in front of everyone else who happens to be in the same "chat room" at the

same time, or very private and personal in the form of person to person instant messages. This communication structure is ideal for the child pornographer. The open and anonymous communication allows the user to locate others of similar inclination and still maintain their anonymity. Once contact is established, it is then possible to send text messages and graphic images to a trusted conspirator. In addition to the use of large service providers, pornographers can use standard internet connections, such as those provided by businesses, universities, and government agencies to communicate with each other and to distribute pornography. These communications links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure and as anonymous as desired. These advantages are well known and are the foundation of commerce between child pornographers.

The computer's ability to store images in digital form makes them an ideal repository for pornography. A compact disk can store hundreds of images and thousands of pages of text. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. Hard drives with a capacity of terabytes are not uncommon. These drives can store many

thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is almost as easy to store an electronic image on a computer located half a world away as it is to store one locally. It is possible to use a camera to capture an image, process that image in a computer and to save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. It is only with careful laboratory examination of electronic storage devices that it is possible to recreate the evidence trail.

The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution of child pornography. This pornography can be electronically mailed to anyone with access to a computer and modem. With the proliferation of commercial services that provide both electronic mail services and chat services, it is no wonder that the computer is the preferred method of distribution of pornographic materials.

#### SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

Based upon your Affiant's knowledge, training and experience, and the experience of other law enforcement

personnel, your Affiant knows that searches and seizures of evidence from computers commonly require agents to seize most or all computer items (hardware, software, and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

Computer storage devices (like hard drives, USB drives, compact disks, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site; and

Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific



procedure which is designed to protect the integrity of the evidence and to recover even "hidden", erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases like this one where the evidence consists partly of graphics files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media). In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crimes of transporting and/or possessing child pornography in violation of law, and should all be seized as such.

## DEFINITIONS

The term "computer", as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

Your Affiant knows that computer hardware and computer software may be utilized to store records which include but are not limited to those relating to business activities, criminal activities, associate names and addresses and the identity and location of assets illegally gained through criminal activity. The terms "records", "documents," and "materials" include all information recorded in any form, including electronic, visual or aural, and including the originals and all non-identical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, including, but not limited to the following:

Written or printed matter of any kind, correspondence, memoranda, notes, diaries, statistics, letters, telephone toll records, telegrams, contracts, reports, checks, statements,

receipts, summaries, pamphlets, books, ledgers, journals, registers, records, vouchers, slips, bills, calendars, pads, notebooks, files, logs, lists, bulletins, credit materials, data bases, teletypes, telefaxes, invoices, worksheets; Graphic records or representations, photographs, slides, drawings, designs, graphs, charts, pictures, sketches, images, films, videotapes; and aural records or representations, tapes, records, discs.

The terms "records", "documents," and "materials" include all of the foregoing in whatever form and by whatever means the records, documents, or materials, their drafts, or their modifications may have been created or stored, including (but not limited to) any handmade form (such as writing, drawing, painting, with any implement on any surface directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); any mechanical form (such as phonograph records, printing, or typing); any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact discs, or any information on an electronic or magnetic storage device, such as floppy diskettes, hard disks, hard drives, CD-ROMs, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic

notebooks, as well as printouts or readouts from any magnetic storage device).

The term "Internet Service Provider" (ISP) refers to an entity which provides access to a host computer, from which electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a dedicated network and serves many users. These host computers are sometimes commercial concerns, such as Charter Communications and AT&T which allow subscribers to connect to a network which is in turn connected to their host systems. These service providers allow electronic mail service between subscribers and sometimes between their own subscribers and those of other networks.

The term "Internet Protocol" (IP) address is a unique identifier for a computer on a network. The format of an IP address is a 32-bit numeric address written as four sequences of numbers separated by periods.

The term "peer-to-peer" (P2P) is a type of network in which each workstation has equivalent capabilities and responsibilities. This differs from client/server architectures, in which some computers are dedicated to serving the others. Peer-to-peer networks are generally smaller, but usually do not offer the same performance under heavy loads.

The term "minor" is defined pursuant to Title 18, United States Code, Section 2256(1), and means any person under the age of eighteen years;

The term "sexually explicit conduct" as used herein is defined pursuant to Title 18, United States Code, Section 2256(2)(A), and means, except as provided in subparagraph (B), actual or simulated--

(i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;

(ii) bestiality;

(iii) masturbation;

(iv) sadistic or masochistic abuse; or

(v) lascivious exhibition of the genitals or pubic area of any person

(B) For purposes of subsection 8(B) of this section, "sexually explicit conduct" means--

(i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited;

(ii) graphic or lascivious simulated;

- (I) bestiality;
- (II) masturbation; or
- (III) sadistic or masochistic abuse; or
- (iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person;

The term "visual depiction", as used herein, is defined pursuant to Title 18, United States Code, Section 2256(5), and includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.

The term "child pornography", as used herein, is defined pursuant to Title 18, United States Code, Section 2256(8), and means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where--

(A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

(B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or:

(C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

The term "child erotica" as used herein, means "any material relating to children, that serves a sexual purpose for a given individual." See Kenneth V. Lanning, Child Molesters: A Behavioral Analysis (2001) at 65. Some of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writings, diaries and sexual aides. Some federal courts have recognized the evidentiary value of child erotica and its admissibility in child pornography cases. United States v. Lamb, 945 F. Supp. 441 (N.D.N.Y. 1996) (child erotica admissible to show defendant's predisposition or lack of mistake); United States v. Cross, 928 F.2d 1030 (11<sup>th</sup> Cir. 1991) (testimony about pedophiles deriving sexual satisfaction from and collecting non-sexual photographs of children admissible to show intent and explain actions of defendant) and United States v. Caldwell, No. 97-5618, 1999 WL 238655 (E.D.KY. Apr. 13, 1999) (child erotica admissible under Federal Rule of Evidence 404(b) to show knowledge or intent).

#### SOURCES OF INFORMATION

On January 25, 2019, a CHS of the Columbia Division of the FBI contacted your affiant and reported that they had found Child Pornography (CP) on a cellular telephone that they had in

their possession. The CHS operates a cellular telephone repair business and as such had obtained this cellular telephone from a customer. Due to the nature of the CHS' business the customer did not provide their full name and contact information. During a check of the cellular telephone to determine if it could be repaired, the CHS found what he believed to be CP. The CHS immediately contacted law enforcement about what was found.

On January 29, 2019, your affiant met with the CHS at their place of employment. The CHS explained that a female customer had come to the shop with a Samsung Model S5 cellular telephone, IMEI [REDACTED], to determine if it could be repaired. The CHS told the customer to check back with him later and he would tell her how much it would cost to repair. When the CHS turned the cellular telephone on they found what appeared to be CP images in the screensaver. The customer had not contacted the CHS about the telephone at that date and to this date has not contacted the CHS.

The CHS then turned on the cellular telephone and allowed the screensaver to come up. The CHS then showed the screen to your affiant. There appeared to be several images of pre-pubescent children engaged in sexually explicit conduct.

Based on this information a Search Warrant was issued in the District of South Carolina for the Samsung Model S5 cellular telephone, IMEI [REDACTED], on February 19, 2019. On March 1, 2019, this search warrant was executed by conducting



a forensic exam on the telephone. The exam found 229 files of suspected CP on the telephone. The exam also revealed that the telephone number associated with this telephone is [REDACTED]. It also revealed the name associated with the telephone is Steven Melton.

On March 11, 2019, your affiant caused an Administrative Subpoena to be served on AT&T, the service provider for telephone number [REDACTED], for subscriber information concerning that number. AT&T responded later that same day providing the following information:

Account Id: [REDACTED]

Subscriber Name: Steven Melton

Service Address: [REDACTED]

[REDACTED]

Email: [REDACTED]

Account Status: Active

Service Start Date: 03/31/2015

South Carolina Department of Motor Vehicles (SCDMV) records lists Steven Jason Melton's address as [REDACTED], South Carolina. SCDMV lists Melton as having three vehicles registered to him or previously registered to him. The address listed for Melton's vehicles is also [REDACTED], South Carolina.

An Accurant database search for Steven Melton lists his address as [REDACTED], South Carolina.

It listed one of his email addresses as [REDACTED].

Accurint also listed telephone number [REDACTED] as assigned to Steven Melton.

Based on my training and experience, my conversations with other more experienced agents, I have learned the following:

Individuals who trade and/or possess child pornography almost always maintain and possess their material in the privacy and security of their homes or some other secure location where it is readily available. The collection may include sexually explicit or suggestive materials involving children, such as photographs, magazines, narratives, motion pictures, video tapes, books, slides, drawings, computer images or other visual media. Individuals who trade and/or possess child pornography are sometimes aroused while viewing the collection and, acting on that arousal, they often masturbate thereby fueling and reinforcing his/her attraction to children. This is most easily accomplished in the privacy of one's own home. Because the collection reveals the otherwise private sexual desires and intent of the possessor and represents his/her most cherished sexual fantasies, the individual rarely, if ever, disposes of the collection. The collection may be culled and refined over time, but the size of the collection tends to increase.

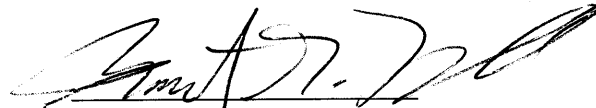
Based on the above information, I believe that there is probable cause to believe that Title 18, United States Code,

Section 2252A(a)(1), which makes it a federal crime for any person to knowingly mail, or transport or ship in interstate or foreign commerce by any means including by computer, any child pornography, and Title 18, United States Code, Section 2252A(a)(5)(B), which makes it a federal crime for any person to knowingly possess any material that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, have been violated.

The property and evidence believed to be concealed at


[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED], authorizing the seizure of the items described in Attachment B.



ROBERT G. HAMOD  
Special Agent  
Federal Bureau of  
Investigation

SUBSCRIBED TO AND SWORN TO  
BEFORE ME THIS FIFTH DAY  
OF APRIL, 2019

  
JACQUELYN D. AUSTIN  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Property to Be Searched**

[REDACTED]

[REDACTED]

is pictured below:

## **ATTACHMENT B**

### **LIST OF ITEMS TO BE SEIZED**

Any cellular telephone, computer, and associated hardware and peripherals, which may be, or are used to visually depict child pornography, information pertaining to the sexual interest in child pornography, sexual activity with children or the transportation or possession of child pornography.

Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data.

Any and all correspondence, electronic or otherwise, pertaining to the transportation or possession of child pornography.

Any and all books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions, electronic or otherwise, of any kind involving the transportation or possession of child pornography, as defined in Title 18, United States Code, Section 2256.